(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

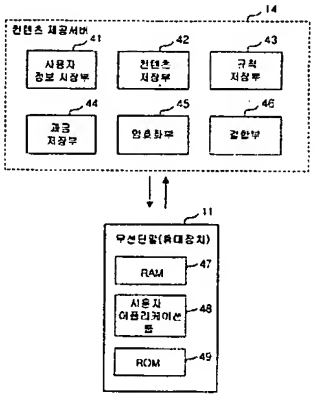
(11)Publication number: 1020040028086 A
(43)Date of publication of application: 03.04.2004

(21)Application number: 1020020059179
(22)Date of filing: 28.09.2002
(30)Priority: ..
(51)Int. Cl G06F 17/00

(71)Applicant: KT CORPORATION
(72)Inventor: PARK, HUN GYU
SEO, SANG YONG

(54) SYSTEM AND METHOD FOR MANAGING CONTENTS COPYRIGHT ON WIRELESS TERMINAL

(57) Abstract:



PURPOSE: A system and a method for managing a contents copyright on a wireless terminal are provided to prevent illegal copy and modify of various kinds of contents used on the wireless terminal. CONSTITUTION: A user information storage (41) stores the user key information and the user information transmitted through a user application tool(48) of the wireless terminal(11). A contents storage(42) stores the contents to be serviced to a user. A rule storage(43) sets a rule such as a storing right, a using period right, and a transfer right. A charge storage(44) confirms a possibility to process the charge for the contents. An encrypting part(45) encrypts the contents requested from the user with an encrypted license key by using a user key. A combiner(46) generates a license decrypting key to decrypt the encrypted license key by combining the charge, the rule, or the user key to the encrypted license key.

Legal Status
Date of request for an examination (20070919)
Notification date of refusal decision (00000000)
Final disposal of an application (application)
Date of final disposal of an application (00000000)
Patent registration number ( )
Date of registration (00000000)
Number of opposition against the grant of a patent ( )
Date of opposition against the grant of a patent (00000000)
Number of trial against decision to refuse ( )
Date of requesting trial against decision to refuse ( )

Date of extinction of right ( )

(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[7]
G06F 17/00

(11) 공개번호 10-2004-0028086
(43) 공개일자 2004년04월03일

(21) 출원번호 10-2002-0059179
(22) 출원일자 2002년09월28일

(71) 출원인 주식회사 케이티
경기 성남시 분당구 정자동 206

(72) 발명자 서상용
서울특별시서초구우면동동양고속아파트105-101

박훈규
서울특별시서초구우면동17

(74) 대리인 특허법인 신성

심사청구 : 없음

(54) 무선단말에서의 컨텐츠 저작권 관리 시스템 및 그 방법

요약

1. 청구범위에 기재된 발명이 속한 기술분야

본 발명은 무선단말에서의 컨텐츠 저작권 관리 시스템 및 그 방법에 관한 것임.

2. 발명이 해결하려고 하는 기술적 과제

본 발명은, 무선단말(개인용 휴대장치)에서 사용되는 각종 컨텐츠의 불법적인 복사 및 변형을 방지하기 위한 무선단말에서의 컨텐츠 저작권 관리 시스템 및 그 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하고자 함.

3. 발명의 해결방법의 요지

본 발명은, 무선단말에서의 컨텐츠 저작권 관리 시스템에 있어서, 컨텐츠 제공서버로부터 사용자 어플리케이션 툴을 다운로드 받아 무선단말에 설치하며, 상기 무선단말의 고유 정보를 이용하여 무선단말 각각의 고유키를 생성하고, 생성된 사용자 고유키 정보를 컨텐츠 제공서버로 전송하기 위한 상기 무선단말; 및 상기 어플리케이션 툴을 통해 사용자 고유키 정보를 수신하여, 사용자 정보, 컨텐츠, 규칙 정보, 과금 정보를 저장하고, 사용자의 요구에 따라 컨텐츠를 사용자 고유키를 이용하여 암호화하여 중계국 및 기지국을 통해 전송하는 컨텐츠 제공서버를 포함함.

4. 발명의 중요한 용도

본 발명은 컨텐츠 저작권 관리 시스템 등에 이용됨.

대표도

도 4

색인어

무선단말, 컨텐츠, 불법복제 방지, 저작권 관리, 사용자 어플리케이션 툴, 암호화된 라이센스, 암호화된 컨텐츠

명세서

도면의 간단한 설명

도 1 은 본 발명이 적용되는 컨텐츠 정보보안 시스템의 구성 예시도.

도 2 는 본 발명에 이용되는 무선단말의 개략적인 구성도.

도 3 은 본 발명에 따른 무선단말에서의 컨텐츠 저작권 관리 시스템 중 암호화된 컨텐츠의 구조를 나타낸 일실시예 설명도.

도 4 는 본 발명에 따른 컨텐츠 제공서버 및 무선단말간의 전송 과정을 나타낸 일실시예 설명도.

도 5 는 본 발명에 따른 무선단말에서의 컨텐츠 저작권 관리 방법 중 무선단말의 고유 아이디 생성 및 인증 과정을 나타낸 일실시예 흐름도.

도 6 은 무선단말에서의 컨텐츠 저작권 관리 방법 중 무선단말을 통해 컨텐츠를 사용하는 과정을 나타낸 일실시예 흐름도.

* 도면의 주요 부분에 대한 부호의 설명

11 : 무선단말 12 : 기지국

13 : 중계국 14 : 컨텐츠 제공서버

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 무선단말에서의 컨텐츠 저작권 관리 시스템 및 그 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것으로, 특히 무선단말(개인용 휴대장치(Presonal mobile device))에서 컨텐츠(Contents)의 저작권 보호를 위해 불법적인 복사 및 변형을 막기 위한 무선단말에서의 컨텐츠 저작권 관리 시스템 및 그 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체에 관한 것이다.

현재, 개인용 휴대장치를 사용하는 사용자는 처음에는 단순히 음성통신만을 이용하였지만 근래에는 데이터 통신도 이용하고 있다. 예를 들면, 개인용 휴대장치는 휴대폰을 이용한 벨소리 다운로드 서비스, 위치정보 제공 서비스, 컴퓨터 없이도 인터넷에 접속이 가능한 인터넷 폰을 이용한 전자메일 처리, 증권 및 열차표 예매와 같은 전자상거래에도 이용되고 있다.

또한, 개인용 휴대장치는 개인용 컴퓨터의 경우와 마찬가지로 운영체계와 중앙처리장치(CPU : Central Processing Unit)에 따라 이미지, 벨소리, 동영상과 같은 다양한 종류의 컨텐츠를 제공하고 있다.

그러나, 개인용 휴대장치에서 제공되는 컨텐츠는 일반적으로 그 크기가 작아 이메일과 같은 수단으로도 배포가 가능하므로, 불법적인 배포에 취약할 수 밖에 없다. 또한, 일반 개인용 컴퓨터나 휴대용 정보 단말기(PDA) 등에서 사용되고 있는 일반적인 암호화 방식이나 인증절차를 핸드폰과 같은 개인용 휴대장치에 사용하고자 하는 경우 저장용량 및 메모리가 극히 제한적이며, 그 수행속도도 떨어지기 때문에 암호화나 인증을 수행하기기가 어렵다. 여기에, 각각의 개인용 휴대장치의 고유번호를 인식할 수가 없고, 개인용 휴대장치의 기종과 운영체제가 통일되어 있지 않기 때문에 개인용 휴대장치에서 실시간으로 사용될 수 있는 암호화 모듈이나 인증절차는 극히 제한적일수 밖에 없다.

또한, 개인용 휴대장치는 그 구성요소가 자체 구동을 위한 기본 프로그램이 내장되어 있는 ROM(Read Only Memory)와 운영체계를 구동하기 위한 플래시 메모리(Flash Memory), 그리고 컨텐츠를 구동하고 저장매체의 역할을 수행하는 RAM(Read Access Memory) 및 컨텐츠를 디스플레이 하기 위한 모니터, 그리고 어플리케이션 및 데이터의 입출력을 위한 입출력 단자 등으로 구성되어 있다.

운영시스템의 경우는 통상 플래시 메모리에 탑재된 형태로 되어 있으며, 컨텐츠나 기존의 데이터 등은 적외선 포트를 통하여 무선으로 전송받거나 혹은 휴대용 입출력 단자를 통해 통상의 개인용 컴퓨터(PC)를 통해서 다운로드받도록 되어있다. 따라서, 대부분의 컨텐츠는 무선을 통해 다운로드 받거나 개인용 PC를 통해서 다운로드 받고 있다. 이 경우 컨텐츠의 업로드나 웹하드, 월드 와이드 웹(WWW : World Wide Web) 등을 통한 불법 어플리케이션의 사용이 용이하기 때문에 이에 대한 대책이 필요한 실정이다.

따라서, 현재에는 이러한 컨텐츠의 보호기술에 대한 요구가 급증하고 있으며, 불법적인 배포 및 사용을 막기 위한 기술과 서비스 분야에 대한 다양한 기술이 개발되고 있다. 이 중 대표적인 것으로는 컨텐츠를 보호하고 보안 및 관리하는 디지털 저작권 관리(DRM : Digital Rights Management) 기술을 들 수가 있다.

DRM 기술은 멀티미디어 정보의 불법유통과 복제를 방지하고, 적법한 사용자만이 정보를 사용할 수 있도록 사용자를 관리하며, 결재 등과 같은 과금서비스를 통해서 멀티미디어 정보의 저작권을 관리하고 있는 기술이다. 이러한 DRM 기술은 현재 시장에서 디지털 정보의 저작권을 보호하고 관리할 수 있는 현실적인 솔루션으로 받아들여지고 있으나, 현재의 DRM 시스템은 그 구조와 시스템이 매우 복잡하고 비대하여 휴대폰과 같은 개인용 휴대기기에는 이를 그대로 적용하여 서비스를 실시하기에는 용이하지 않은 문제점이 있다. 또한, 이러한 개인용 휴대장치는 소형화나 전력문제 등을 고려하는 이유로 통상의 정보는 개인용 컴퓨터나 PDA상에서 표시되는 것에 비해 매우 간소화되어 통상의 DRM에 적용되는 암호화 알고리즘등을 개인용 휴대장치에 그대로 적용시 계산속도나 전력문제가 발생하기 때문에 이로 인한 컨텐츠의 원활한 사용이 어려운 문제점이 있다.

발명이 이루고자 하는 기술적 과제

본 발명은, 상기한 바와 같은 문제점을 해결하기 위하여 제안된 것으로, 무선단말(개인용 휴대장치)에서 사용되는 각종 컨텐츠의 불법적인 복사 및 변형을 방지하기 위한 무선단말에서의 컨텐츠 저작권 관리 시스템 및 그 방법과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는데 그 목적이 있다.

발명의 구성 및 작용

상기 목적을 달성하기 위한 본 발명은, 무선단말에서의 컨텐츠 저작권 관리 시스템에 있어서, 컨텐츠 제공서버로부터 사용자 어플리케이션 툴을 다운로드 받아 무선단말에 설치하며, 상기 무선단말의 고유 정보를 이용하여 무선단말 각각의 고유키를 생성하고, 생성된 사용자 고유키 정보를 컨텐츠 제공서버로 전송하기 위한 상기 무선단말; 및 상기 어플리케이션 툴을 통해 사용자 고유키 정보를 수신하여, 사용자 정보, 컨텐츠, 규칙 정보, 과금 정보를 저장하고, 사용자의 요구에 따라 컨텐츠를 사용자 고유키를 이용하여 암호화하여 중계국 및 기지국을 통해 전송하는 컨텐츠 제공서버를 포함하여 이루어진 것을 특징으로 한다.

또한, 본 발명은, 무선단말에서의 컨텐츠 저작권 관리 시스템에 있어서, 컨텐츠 제공서버와 무선단말과의 전송과정을 통해 상기 컨텐츠 제공서버로부터 사용자 어플리케이션 툴을 다운로드 받아 무선단말에 설치하며, 상기 무선단말의 고유정보를 이용하여 해당 사용자의 고유키를 생성하기 위한 고유키 생성수단; 상기 고유키 생성수단을 통해 사용자 고유키 정보를 추출하기 위한 추출수단; 및 상기 고유키 생성수단으로부터 다운받은 컨텐츠를 저장하기 위한 저장수단을 포함하여 이루어진 것을 특징으로 한다.

또한, 본 발명은, 무선단말에서의 컨텐츠 저작권 관리 시스템에 있어서, 상기 사용자 어플리케이션 툴을 통해 전송된 사용자 고유키 및 사용자 정보를 저장하기 위한 사용자 정보 저장수단; 사용자에게 서비스하는 대상 컨텐츠를 저장하기 위한 컨텐츠 저장수단; 사용자의 권한에 따른 저장권한, 사용기간 권한, 양도권한 등 과 같은 규칙을 설정하는 규칙 저장수단; 사용자의 컨텐츠 사용에 대한 권한으로, 컨텐츠에 대한 대가 처리 가능성 여부를 확인하고 과금 등의 처리를 수행하는 과금 저장수단; 사용자에 의해 요청된 컨텐츠를 사용자의 고유키를 사용하여 암호화된 라이센스로 암호화하기 위한 암호화수단; 및 상기 암호화수단에서 암호화된 라이센스 키(key)에 과금이나, 규칙, 사용자 고유키를 결합하여 암호화된 라이센스 키를 복호화하기 위한 라이센스 복호화 키를 생성하는 결합수단을 포함하여 이루어진 것을 특징으로 한다.

또한, 본 발명은, 컨텐츠 저작권 관리 시스템에 적용되는 무선단말에서의 컨텐츠 저작권 관리 방법에 있어서, 사용자가 컨텐츠 제공서버에 접속시, 해당 사용자 무선단말로 사용자 어플리케이션 툴을 설치하고, 상기 사용자 무선단말의

고유정보를 이용하여 생성된 사용자 고유키를 사용자 어플리케이션에서 추출하는 제 1 단계; 상기 사용자 고유키를 상기 컨텐츠 제공서버로 전송하는 제 2 단계; 사용자로부터 컨텐츠 다운로드 요청시, 해당 컨텐츠를 사용자 고유키를 통하여 암호화하고, 암호화된 컨텐츠 패키지를 생성하는 제 3 단계; 상기 암호화된 컨텐츠 패키지를 다시 사용자 고유정보를 통해서 암호화된 컨텐츠로 암호화하고, 암호화된 컨텐츠를 상기 무선단말로 전송하는 제 4 단계; 인증된 사용자의 무선단말에서 상기 암호화된 컨텐츠를 사용자 고유정보를 통해서 암호화된 컨텐츠 패키지로 복호화하는 제 5 단계; 및 상기 암호화된 컨텐츠 패키지를 사용자 고유키를 통해 컨텐츠로 복호화하고, 복호화된 컨텐츠를 상기 무선단말을 통해 출력하는 제 6 단계를 포함하여 이루어진 것을 특징으로 한다.

또한, 본 발명은, 프로세서를 구비한 컨텐츠 저작권 관리 시스템에, 사용자가 컨텐츠 제공서버에 접속시, 해당 사용자 무선단말로 사용자 어플리케이션 툴을 설치하고, 상기 사용자 무선단말의 고유정보를 이용하여 생성된 사용자 고유키를 사용자 어플리케이션에서 추출하는 제 1 기능; 상기 사용자 고유키를 상기 컨텐츠 제공서버로 전송하는 제 2 기능; 사용자로부터 컨텐츠 다운로드 요청시, 해당 컨텐츠를 사용자 고유키를 통하여 암호화하고, 암호화된 컨텐츠 패키지를 생성하는 제 3 기능; 상기 암호화된 컨텐츠 패키지를 다시 사용자 고유정보를 통해서 암호화된 컨텐츠로 암호화하고, 암호화된 컨텐츠를 상기 무선단말로 전송하는 제 4 기능; 인증된 사용자의 무선단말에서 상기 암호화된 컨텐츠를 사용자 고유정보를 통해서 암호화된 컨텐츠 패키지로 복호화하는 제 5 기능; 및 상기 암호화된 컨텐츠 패키지를 사용자 고유키를 통해 컨텐츠로 복호화하고, 복호화된 컨텐츠를 상기 무선단말을 통해 출력하는 제 6 기능을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

본 발명은, 정보단말기의 컨텐츠에서 저작권 관리를 적용하기 위하여 필요로 하는 사용자의 고유키 및 사용자 고유정보, 그리고 이를 통한 암호화된 라이센스 및 암호화된 컨텐츠를 생성하는 것을 특징으로 한다.

또한, 본 발명은, 사용자의 고유키를 생성하고 암호화하기 위한 컨텐츠 제공서버의 운영방식을 제공하며, 사용자 어플리케이션 툴을 사용하여 사용자의 고유키 및 사용자 고유정보를 인증하는 방법과 암호화된 컨텐츠를 사용자 어플리케이션 툴을 통하여 복호화하는 것을 특징으로 한다.

상술한 목적, 특징들 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일실시예를 상세히 설명한다.

도 1 은 본 발명이 적용되는 컨텐츠 정보보안 시스템의 구성 예시도이다.

도 1에 도시된 바와 같이, 본 발명이 적용되는 컨텐츠 정보보안 시스템은, 무선단말(11), 기지국(12), 중계국(13), 컨텐츠 제공서버(14)의 네 부분으로 크게 구분된다.

통상적으로, 무선단말(11)을 통한 서비스는 무선단말(11)에서 데이터의 입력에 의해 생성된 데이터가 무선으로 통신을 하는 송수신 제어장치에 의하여 통신을 하는 통신장치에 의해 기지국(12)과 통신을 하고, 기지국(12)을 통해 송신된 데이터가 중계국(13)으로 수신되어 컨텐츠 제공서버(14)를 통해 서비스 되고자 하는 대상에 접속하여 전송된 데이터에 의하여 실행프로그램이 작동하고, 다시 컨텐츠 제공서버(14)에서 실행프로그램의 수행에 따른 실행결과가 중계국(13) 및 기지국(12)을 거쳐 무선단말(11)에 수신되어 서비스가 이루어지는 구조로 되어 있다.

여기서, 기지국(12)은 다수의 통신방식에 의한 통신이 가능하도록 되어, 만일 어느 한 기지국과의 통신에 실패하였을 때 다수의 통신장치 중 다른 통신장치에 의해 기지국(12)과의 통신을 수행하도록 되어 있으며, 장거리 무선랜(W-LAN)에 의해 기지국(12)과 통신을 하는 장거리 통신장치와, 단거리 무선랜에 의해 기지국(12)과 통신을 하는 단거리 통신장치로 구성된다. 이외에 다른 통신방식에 의해 기지국(12)과 통신을 하는 다수의 통신장치를 접속하는 것도 가능하다.

그리고, 중계국(13)에는 무선단말(11)과 무선통신을 행하는 다수의 기지국이 접속되어 있고, 중계국(13)은 무선단말(11)이 컨텐츠 제공서버(14)를 통해, 예를 들면 인터넷이나 벨소리 다운로드 서비스와 같은 특정서비스에 접속될 때, 무선단말(11)을 대신하여 기지국(12)을 통해 수신한 무선단말(11)로부터의 데이터를 인터넷을 통해 목적으로 하는 장치에 송신함과 동시에, 컨텐츠 제공서버(14) 상의 서비스를 목적으로 하는 단말의 데이터를 기지국(12)을 통해 무선단말(11)에 송신하도록 되어 있다.

또한, 무선단말(11)은 적어도 3개의 기지국과 동시에 통신을 하도록 되어 있고, 중계국(13)은 무선단말(11)로부터의 전파가 각 기지국에 도달하기까지의 시간의 각각의 시간차를 측정하여, 측정한 시간차에 따라 무선단말(11)의 위치를 측정하는 위치측정 서비스(Global Positioning Service:GPS) 등을 제공해준다.

도 2 는 본 발명에 이용되는 무선단말의 개략적인 구성도이다.

도 2에 도시된 바와 같이, 무선단말(휴대장치)(11)은, 제어 프로그램에 의하여 연산 및 휴대장치의 시스템 전체를 제

어하는 중앙처리(CPU : Central Processing Unit)부(21)와, 휴대장치의 소정영역에 CPU의 제어 프로그램을 포함하고 있는 ROM(Read Only Memory)부(22)와, ROM부(22)로부터 읽어낸 데이터나 컨텐츠, CPU의 연산과정에서 필요한 연산결과를 저장하기 위한 RAM(Random Access Memory)부(23)와, RAM의 특정영역에 저장되어 있는 데이터나 컨텐츠를 어드레스를 통해 소정 주기에 따라 순차 판독하고, 읽어낸 표시용 데이터를 화상신호로 다시 변환하여 출력하기 위한 CRT부(24)와, CPU부(21), ROM부(22), RAM부(23), CRT부(24)로부터 데이터를 받아서 전송하기 위한 버스(26)와, 외부장치인 입력부(27), 제어부(28), 표시부(29)에 대한 입출력을 매개하는 인터페이스부(25)와, 휴먼 인터페이스로서 다수의 키에 의해 데이터의 입력이 가능한 입력부(27)와, 인터페이스부(25)를 통해 전송되는 데이터나 신호에 따라 무선단말(11)을 제어하는 제어부(28)와 화상신호에 따라 화면을 표시하는 표시부(29)를 구비한다.

여기서, CPU부(21)는 마이크로 프로세싱 유닛(MPU) 등으로 이루어지고, ROM의 소정영역에 저장되어 있는 소정의 프로그램을 구동시키고, 그 프로그램에 따라 데이터 제어 처리를 실행하는 연산을 수행하도록 한다.

ROM부(22)는 비휘발성 메모리로 통상의 휴대장치(11)에서 서비스하기 위한 기기의 제어를 위한 프로그램과 운영 시스템 등을 포함하고 있으며, 이를 통해 휴대장치(11)를 구동하도록 한다.

RAM부(23)는 ROM부(22)의 프로그램을 통해 실행가능한 서비스를 위한 어플리케이션 프로그램이나 이를 통해 서비스되는 각종 컨텐츠를 저장하는 역할을 담당한다.

CRT부(24)는 ROM부(22)에서 휴대장치의 서비스를 위한 각종 기능을 수행하거나 입력부를 통해 데이터를 입력하는 등의 제어절차를 인터페이스부(25)를 통해 일정 어드레스로 전달해준다.

인터페이스부(25)는 전송되는 각종 데이터나 제어신호를 전송하는 역할을 담당한다.

입력부(27)는 사용자의 필요에 따라 데이터나 혹은 제어신호를 입력하는 역 할을 담당하며, 표시부(29)를 통해 사용자가 그 입력사항을 확인하도록 한다.

제어부(28)는 CRT부(24)에서 발생한 제어신호 등을 음성전달 장치인 송화부 및 수화부를 통해 전달해주는 역할을 한다.

표시부(29)는 휴대장치(11)에서 송수신되는 데이터 및 제어여부를 LCD(Liquid Crystal Display) 패널과 같은 형태를 통해 화상신호에 따라 화면을 표시하거나 입출력 매개상태를 확인하도록 한다.

본 발명에 따르면, 휴대장치(11)에서 컨텐츠에 대한 불법적인 복사 및 변형을 방지하기 위한 저작권 관리 방법의 실시를 위해서는 ROM부(22)의 메모리를 사용하는 것이 효과적이지만, 이는 초기에 휴대장치(11)를 배급하는 회사에 의해 세팅되기 때문에 사용하기가 어렵다.

따라서, 본 발명에서는 ROM부(22)에 기록되어 있는 소정의 정보를 사용하여 RAM의 소정영역에 이를 저장하고, CRT부(24) 및 제어부(28)를 제어한다. 또한, RAM부(23)에 저장됨으로써 악의의 목적을 가진 사용자에 의하여 본 발명의 실시를 방해하는 것을 방지하기 위하여 컨텐츠를 암호화하여 제공한다.

이를 위하여, 사용자의 휴대장치(11)의 고유 정보를 사용하여 휴대장치 각각의 고유키를 생성하여 서비스를 위한 사용자 등록시 사용자 어플리케이션 툴을 제공하고, 이를 휴대장치(11)에서 실행하도록 함으로써, 고유의 개인키를 컨텐츠 제공서버(14)로 송신한다. 상기 과정에서 발생하는 컨텐츠의 사용에 대한 인증과 관련하여, 사용자 어플리케이션 툴은 각종 사용 가능한 조건 및 사용자 고유키를 컨텐츠 제공서버(14)에 제공하고, 이 조건에 대한 자료 또는 신호를 전송한다.

이에 따라, 컨텐츠 제공서버(14)는 사용자 고유키 정보를 사용자 어플리케이션 툴로부터 전송받아 사용자를 제어하기 위한 각종 규칙이나, 서비스 내역 등을 확인한다.

상기에서 설명한 사용자 어플리케이션 툴은 기출원된 발명(디지털 컨텐츠의 보호 및 관리를 위한 방법 및 이를 이용한 시스템 : 특허 출원번호 제 2001-23562호(2001. 4. 30))의 CCR(Contents Control Region) 등을 통해 보다 상세히 개시되어 있다.

상기 출원된 발명에 따르면 시스템 고유 정보에 의한 사용자 고유 키 생성은 이러한 각 사용자의 시스템 구성 요소들의 고유 정보를 토대로 사용자 고유 키를 생성하며, 이를 통해 사용자 인증 및 정보 사용 재생 여부를 제어한다.

보다 상세히 설명하면, 중앙처리장치의 경우 펜티엄 Ⅲ 이상의 칩은 고유 ID를 가지고 있다. 또한 하드디스크는 그 마스터 영역의 물리적인 섹터를 조사하면 제조사 정보(IDE)를 찾을 수 있다. 이와 같이 시스템의 특성들을 나타내는 정

보들을 추출하며, 이렇게 추출된 시스템 고유 정보를 근거로 사용자 고유 키를 생성한다.

이러한 추출된 고유 정보를 외부적으로 확인할 수 없도록 차단하는 기능을 가지는 사용자 애플리케이션 툴에서 공지의 블랙박스에 저장한 후, 이러한 고유 정보를 이용하여 사용자 고유 키를 생성한다. 생성된 사용자 고유 키는 보안유지를 위하여 레지스트리(registry)등에는 남아있지 않도록 하며 제공하는 사용자 애플리케이션 툴에서 정보를 요청할 때마다 사용자 고유키를 검색하여 암호화된 정보를 풀어준다. 물론 이 플러그 인에는 블랙박스가 내장되어 있도록 한다. 이상과 같은 일련의 과정에 의하여 특정 사용자가 인증한 정보는 규칙설정부(142)에서 정한 규칙에 의하여 제2, 제3의 사용자에게 재배포되어 인증된 허가없이 재사용될 수 없도록 제어되는 것을 특징으로 한다.

한편, 상기 사용자 어플리케이션 툴에서 휴대장치 사용자의 고유키 생성 동작을 보다 상세히 설명하면, 휴대장치를 구성하는 요소들로는 도 2에 나타난 바와 같이 각종 장치부로 구성되어 있다. 본 발명에 따른 휴대장치에서의 컨텐츠 저작권 관리 시스템의 고유정보에 의한 사용자 고유 키 생성은 이러한 각 사용자의 휴대장치 구성요소들의 고유정보를 이용하여 사용자 고유키를 생성하며, 이를 통해 사용자 인증 및 컨텐츠 사용을 위한 암호화 및 복호화 여부를 제어한다.

보다 상세히 설명하면, 휴대장치의 CPU의 경우, 고유의 ID를 가지고 있다. 또한, RAM을 포함하고 있는 메모리 칩의 경우 그 마스터 영역의 물리적인 섹터를 조사하면 제조사 정보(IDE)나 고유의 ID 등을 찾을 수 있다. 제조사 정보에는 제조사명, 시리얼 번호 등에 대한 정보가 포함되어 있다. 본 발명에서는 이와 같이 시스템의 특성들을 나타내는 정보들을 추출하여, 이렇게 추출된 고유정보를 근거로 사용자 고유키의 일부를 생성한다.

여기서, 휴대장치는 일반 개인용 컴퓨터(PC)와는 달리 사용자의 요구나 필요에 따라 특정정보, 예를 들면 사용자의 명의변경에 의하여 사용자의 정보가 변경되거나 혹은 사용자가 전화번호를 변경하는 등의 변경사항이 발생할 수가 있다. 따라서, 이러한 정보변경에 따른 고유정보의 변경에 따른 문제를 해결하기 위하여 사용 자의 전화번호를 고유정보로 사용하되, 이에 따른 데이터의 관리는 서비스 제공서버나 혹은 통신 서비스 제공업체의 데이터베이스와의 연동을 통해 그 변경사항을 추적하도록 한다. 본 발명에서는 사용자의 서비스를 위한 사용자 인증시 전송되는 사용자의 전화번호와 사용자 어플리케이션 툴을 통해 생성된 고유정보를 결합하여 사용자 고유키를 생성하고 암호화된 컨텐츠 전송시에 사용자 어플리케이션 툴을 통해 전화번호와 사용자 고유정보를 복호화키로 사용하여 컨텐츠를 복호화한다.

또한, 사용자 어플리케이션 툴에서는 상기 추출된 고유키를 외부적으로 확인할 수 없도록 차단하는 기능을 가지는 사용자 어플리케이션 툴에서 공지의 블랙박스에 저장한 후, 이러한 고유정보를 이용하여 사용자 고유키를 생성한다. 생성된 사용자 고유키는 보안유지를 위하여 본 발명에서 제공하는 사용자 어플리케이션 툴에서 정보를 요청할 때마다 사용자 휴대장치의 정보를 검색하여 고유키를 생성한다. 이상과 같은 일련의 과정에 의하여 특정 사용자가 인증한 정보는 서비스 제공서버에 전송되어 각종 규칙이 설정되어 제2, 제3의 사용자에게 재배포되어 인증된 허가없이 재사용되는 것이 제어된다.

또한, 사용자 어플리케이션 툴은, 초기 설치시와 해당 사용자 무선단말의 업그레이드나 정보변경시, 상기 사용자 고유정보를 추가적으로 전송한다.

이렇게 생성된 사용자 고유 키는 컨텐츠 제공서버에 전달되어 본 발명에 따른 서비스를 이용하는 사용자들에 대한 정보로서 관리된다.

상기에서와 같이, 사용자 정보를 이용한 사용자 고유키의 전송을 통한 사용자의 정보가 컨텐츠 제공서버에 저장되면, 사용자의 요구에 의하여 컨텐츠 제공서 버에서 컨텐츠를 사용자 고유키를 이용하여 암호화하여 중계국 및 기지국을 통해 송신함으로써, 해당 사용자는 암호화가 이루어진 컨텐츠를 인증절차를 거쳐서 전달받게 된다.

본 발명에서 암호화된 정보를 복호화하는 키는 사용자에게 전송되는 것이 아니라 사용자 어플리케이션 툴을 통해 휴대장치 고유의 정보를 통해 관리되도록 함으로써, 그 보안성을 높여 복호화키가 유출되는 것을 방지하도록 한다.

컨텐츠에 적용되는 암호화키는 소정크기의 바이트 길이를 갖는(본 발명의 일 실시예에서는 128비트의 길이를 가지는) 암호화 키가 이용될 수 있다. 이러한 암호화에는 상용화된 다양한 암호화 알고리즘을 사용할 수 있으며, 그 예로 타원형 곡선 알고리즘과 같은 블록형 알고리즘, 또는 RC4와 같은 스트림 알고리즘 등을 예로 적용할 수 있다.

사용자는 컨텐츠를 사용하기 위해서만 키를 이용하며, 정보는 항상 존재하는 것이 아니고 사용시에만 사용자 어플리케이션 툴을 통하여 사용자 고유정보를 추출하여 컨텐츠 암호화 키의 인증을 통해서 사용 가능한 형태로 제공되며 사용후에는 RAM에서 제거된다.

또한, 사용자 고유정보는 휴대장치 고유번호, 무선전화기 식별번호(MIN : Mobile Identification Number)나 단말기 고유번호(ESN : Electronic Serial Number)와 같은 브라우저 ID 정보를 이용한다. 통상적으로, 핸드폰의 전원이 켜

지면 핸드폰은 가까운 기지국으로 MIN과 ESN메시지를 보내고, 기지국은 이 메시지를 교환기로 보내게 된다. 이때, 교환기는 받은 MIN(전화번호)을 네트워크 안의 모든 MIN과 비교해 해당 휴대폰이 홈 교환국 위치인지 방문자 교환국 위치인지를 판별한다. 이때, 홈위치등록기(HLR : Home Location Resister)는 해당 휴대폰의 정보를 요구하게 된다. 만일, 해당 휴대폰이 외부에 있경우 교환기는 STP(Signaling Transfer Point: 신호 전송 포인트)에 저장된 라우팅 정보(추적 루트)를 이용하여 그 가입자가 속해 있는 HLR로 메시지를 보내게 된다. 이때, HLR는 이 신호를 받아 MIN과 ESN을 이용해 번호가 유효한지 불법으로 쓰는지를 확인한 후 위치정보를 HLR에 등록하고 해당 휴대폰 정보를 외부 방문 교환국으로 보낸다. 이때, 외부 방문 교환국에서는 이를 수신해 이를 방문자위치등록기(VLR)에 저장해 이용자는 홈 위치 이외의 곳에 있는 동안 홈교환국을 거칠 필요없이 통화를 받을 준비를 하게 된다.

따라서, 휴대장치를 이용하기 위해서는 MIN이나 ESN의 사용이 필수적이기 때문에 이를 사용자 고유정보로 사용하는 것이 가능하다.

도 3 은 본 발명에 따른 무선단말에서의 컨텐츠 저작권 관리 시스템 중 암호화된 컨텐츠의 구조를 나타낸 일실시예 설명도이다.

도 3에 도시된 바와 같이, 암호화된 컨텐츠는 헤더부(31), 컨텐츠부(32), 컨텐츠 키(key)부(33)과 같이 구성되며, 헤더부(31)에는 사용자 정보, 사용자 기기정보등이 포함되거나 혹은 해당 사용자 정보와 컨텐츠 제공서버를 통해 다른 사람에게 컨텐츠를 제공하고자 할 경우 특정 사용자의 전화번호와 같은 사용자 정보가 포함될 수 있다.

컨텐츠부(32)는 컨텐츠 제공서버에서 사용자에게 제공하고자 하는 특정 컨텐츠로써, 이미지 파일(GIF나 TIF 등), 음원 파일(MP3나 WMA, AAC, WAV 등), 영상 파 일(DIVX나 WMV 등) 및 기타 다양한 형태의 컨텐츠의 사용이 가능하다.

컨텐츠 키(Key)부(33)는 휴대장치로부터 얻어진 사용자 고유키를 이용하여 컨텐츠부(32)의 컨텐츠와 동일한 길이와 동일한 형태로 생성하기 위하여 매우 긴 주기의 난수열을 발생시켜 제작된다. 이 컨텐츠 키(key)부(33)를 통하여 암호화된 컨텐츠부(32)가 복호화된다.

이렇게 암호화된 라이센스부는 다시 상기 설명한 MIN이나 ESN과 같은 사용자 고유정보 및 과금여부등이나 컨텐츠의 제한사항을 규정한 규칙 등과 결합하여 암호화된 라이센스를 복호화할 수 있는 키로써 암호화된 라이센스와 결합하여 암호화된 컨텐츠를 생성한다.

상기 암호화된 컨텐츠에 적용되는 암호화된 라이센스의 복호화 키는 사용자 고유정보를 포함한 규칙정보 등을 사용하여 구성되며, 소정크기의 바이트 길이를 갖는 암호화 키가 이용될 수 있다. 이러한 암호화에는 NIST의 공인 알고리즘이나 상용화된 다양한 암호화 알고리즘을 사용할 수 있다. 또한, 상기에서 설명된 암호화된 컨텐츠를 복호화하기 위하여 사용된 사용자 고유키를 사용하여 라이센스 키를 암호화하기 위하여 사용한 알고리즘을 그대로 사용하는 것도 가능하다.

도 4 는 본 발명에 따른 컨텐츠 제공서버 및 무선단말간의 전송 과정을 나타낸 일실시예 설명도이다.

도 4에 도시된 바와 같이, 휴대장치(11)는 컨텐츠 제공서버(14)와 휴대장치(11)와의 전송과정을 통해 컨텐츠 제공서버(14)로부터 다운로드 받은 사용자 어플리케이션 툴(48)과, 사용자 고유키 정보를 추출하기 위한 ROM(49), 그리고 상기 사용자 어플리케이션을 통해 다운받은 컨텐츠를 저장하기 위한 RAM(47)을 포함한다.

또한, 컨텐츠 제공서버(14)는 휴대장치(11)의 사용자 어플리케이션을 통해 전송된 사용자 고유키 및 사용자 정보를 저장하는 사용자 정보 저장부(41)와, 사용자에게 서비스하는 대상 컨텐츠를 저장하는 컨텐츠 저장부(42)와, 사용자의 권한에 따른 저장권한, 사용기간 권한, 양도권한 등과 같은 규칙을 설정하는 규칙 저장부(43)와, 사용자의 컨텐츠 사용에 대한 권한으로서, 컨텐츠에 대한 대가 처리 가능성 여부를 확인하고 과금 등의 처리를 수행하기 위한 과금 저장부(44)와, 사용자에 의해 요청된 컨텐츠를 사용자의 고유키를 사용하여 암호화된 라이센스로 암호화하는 암호화부(45) 및 상기 암호화된 라이센스키에 과금이나, 규칙, 사용자 고유키를 결합하여 암호화된 라이센스 키를 복호화하기 위한 라이센스 복호화키를 생성하는 결합부(46)를 포함한다.

휴대장치(11)는 컨텐츠 제공서버(14)로부터 다운로드 받은 사용자 어플리케이션 툴(45)과 사용자 고유키 정보를 추출하기 위한 ROM(49)에서 사용자의 고유키를 추출하며, 상기 고유키에 대한 설명은 상기 도 3에서 설명한 바와 같다.

이렇게 추출된 사용자 고유키는 휴대장치(11)의 RAM(47)에 저장되지 않고 컨텐츠 제공서버(14)로 전송되어 사용자 정보 저장부(41)에 사용자의 일반정보와 같이 저장된다. 이후, 컨텐츠 제공서버(14)는 사용자의 정보를 토대로 사용자에 대한 권한 등을 정하여 규칙 저장부(43)에 저장하고 사용자의 과금에 대한 처리능력 등을 과금 저장부(44)에 저

장한다.

사용자의 요구에 의하여 컨텐츠를 전송하여야 하는 경우에는 컨텐츠 제공서버(14)는 과금 저장부(44) 및 사용자 정보 저장부(41)를 통하여 사용자의 신상정보와 컨텐츠 제공능력을 체크하게 되며, 상기 과정에서 정당한 사용자임이 확인되면, 컨텐츠 제공서버(14)는 대상 컨텐츠를 컨텐츠 저장부(42)에서 불러들여 사용자 정보 저장부(41)에서 읽어들인 사용자 고유정보로 암호화하고, 규칙과 과금에 관련한 사항을 규칙 저장부(43)와 과금 저장부(44)에 저장한 후에 상기 정보를 결합부(46)에서 헤더부에 결합하여 암호화된 컨텐츠를 생성하여 휴대장치(11)로 전송한다.

휴대장치(11)로 전송된 암호화된 컨텐츠는 사용자 어플리케이션 툴에서 사용자 고유정보와 일치여부를 확인하고(이것은 통화가 시작되면 MIN과 ESN을 통해 확인이 가능함을 상기에서 설명하였음), 정당한 사용자임이 확인되면 암호화된 컨텐츠를 사용자 어플리케이션 툴에서 라이센스 복호화키와, 규칙, 암호화된 라이센스로 풀리게 되고, 이 암호화된 라이센스를 복호화하기 위한 라이센스 복호화키를 통하여, 암호화된 컨텐츠 및 사용자 고유키로 암호화된 컨텐츠 복호화키를 추출하여 RAM(47)에 저장하고, 여기서 사용자 어플리케이션을 통한 컨텐츠의 복호화를 실시하여 사용자 고유키를 사용하여 암호화된 컨텐츠를 복호화한 후에 이를 화면상에 출력하여 서비스한다.

도 5 는 본 발명에 따른 무선단말에서의 컨텐츠 저작권 관리 방법 중 무선단말의 고유 아이디 생성 및 인증 과정을 나타낸 일실시예 흐름도이다.

도 5에 도시된 바와 같이, 사용자가 휴대장치에서 무선으로 혹은 웹을 통하여 인터넷에 접속하여 컨텐츠 제공서버에 접속되면(501), 사용자가 등록되었는지를 확인하여(502) 이미 등록되었으면 컨텐츠 제공서비스와 같은 해당 기능을 수행하고(503), 등록되지 않았으면 사용자가 상기 서비스를 이용할 권리가 있는 적합한 사용자인지를 컨텐츠 제공서버와 연동된 데이터베이스를 통하여 확인한다(504).

확인결과, 부적합한 사용자일 경우 사용자가 서비스를 이용하도록 요구하거나 부적합한 사용자로 처리하며(505), 적법한 사용자일 경우 컨텐츠 제공서버에서 사용자 어플리케이션 툴을 다운로드하여 설치한다(506). 또는, 컨텐츠 제공서버에서 사용자의 정보일부가 포함된 실행파일을 내려줌으로써 추가적으로 사용자 어플리케이션 툴의 불법복제를 막는 것도 가능하다. 상기 과정을 통하여 사용자의 휴대장치로 다운로드된 사용자 어플리케이션의 실행을 통하여 사용자 휴대장치로부터 사용자 고유키가 컨텐츠 제공서버로 전송된다(507). 이렇게 함으로써 휴대장치에서 사용자의 등록은 완료되며(508) 사용자 휴대장치로부터 전송된 사용자 고유키를 컨텐츠 제공서버의 사용자 정보서버에 저장함으로써 사용자 등록이 완료되게 된다(509).

도 6 은 무선단말에서의 컨텐츠 저작권 관리 방법 중 무선단말을 통해 컨텐츠를 사용하는 과정을 나타낸 일실시예 흐름도이다.

도 6에 도시된 바와 같이, 사용자에게 필요한 컨텐츠를 제공하기 위하여, 사용자가 웹이나 서버에 접속하면(601), 사용자가 등록되었는지를 확인한다(602).

여기서, 컨텐츠 제공서버는 사용자의 등록여부를 체크하여 웹상에서 등록을 수행하도록 한다. 만일 등록이 되어 있지 않은 사용자일 경우에는 컨텐츠 제공서버 와 연동된 사용자 정보서버에 등록여부를 MIN이나 ESL을 통해 체크하고((509)과정) 등록하지 않은 경우에는 (603)과정에서 사용자 미등록 등의 경고를 사용자의 휴대장치에 전송하여 화면에 출력되도록 한 후 (502)과정으로 진행하고 등록하는 경우에는 (504)과정에서 등록절차를 밟아 등록하도록 한다. 등록 후에는 (602)과정에서 다시 MIN이나 ESL을 통해 등록이 되었는지 확인하여 등록되지 않았을 경우나 혹은 에러가 발생한 경우에는 (504)과정을 다시 거치도록 하고 이상이 없을 경우는 (604)과정으로 진행한다.

(604)과정에서는 컨텐츠를 제공하기에 적합한 사용자인지 확인하는 과정을 나타낸 것이다.

(604)과정에서는 사용자의 휴대장치에서 사용자 어플리케이션 툴을 통해 사용자의 고유정보나 고유키에 대한 정보를 컨텐츠 제공서버로 전송하고, 이를 통하여 컨텐츠 제공서버에서 사용자의 정보와 비교하여 사용자에게 컨텐츠를 전송할 준비를 완료한다. 만일, 이 과정에서 사용자 어플리케이션 툴을 통해 전송된 사용자의 고유정보나 고유키에 대한 정보가 개인용 휴대장치의 사용자 정보와 일치하지 않은 경우에는 사용자 휴대장치의 출력부(화면)에 시스템상의 이상을 표시해 줄 수 있다(일반적인 상황에서는 이전에 (508)과정에 의해 이미 사용자 고유키가 생성되어야 하기 때문에, 이 상황이 발생하면 크랙킹(Cracking) 혹은 시스템 문제가 발생한 것으로 판단할 수 있다).

만일, 읽어 들이기가 실패하거나 사용자의 정보와 일치하지 않을 경우는 (605)과정로 진행한다.

사용자의 정보가 일치하는 경우는 컨텐츠 제공서버에서 사용자 정보 서버에 저장된 사용자 고유정보와 사용자 고유키를 불러들여 사용자 고유키를 이용하여 컨텐츠를 암호화하여 헤더부에 사용자 고유정보 및 규칙등을 추가하고(607) 사용자의 휴대장치로 송신한다(608).

마지막으로, 휴대장치의 인터페이스부를 통해 암호화된 컨텐츠가 올바르게 전송되었는지 확인한다. 만일, 올바르게 전송되지 않는 경우는 상기와 마찬가지로 (604)과정으로 진행한다.

사용자 고유정보에는 MIN과 ESL외에도 다른 정보가 삽입되는 것이 가능하다. 이 경우, 크게 3가지의 정보가 들어가는 것이 가능한데, 첫째로 정상적으로 복호화가 되어 있는지 확인할 수 있는 확인정보, 둘째로 소프트웨어 제조사가 원하는 정보, 예를 들면 사용자 ID, 시리얼 넘버(Serial Number), 사용등급, 소프트웨어 레벨(Level), 사용자 전화번호, 혹은 사용자가 다른 사용자에게 컨텐츠를 제공하는 경우 다른 사용자의 사용자 전화번호 등의 정보, 세째로 이 정보의 변형을 확인할 수 있는 CRC같은 정보와 함께 암호화된 정보를 말한다.

(609)과정은 사용자 휴대장치로 전송된 암호화된 컨텐츠 정보가 사용자 어플리케이션 툴을 통해 사용자의 고유정보와 사용자 고유키를 확인하는 과정이다. 사용자 어플리케이션 툴을 통해 헤더부의 정보와 컨텐츠 키(KEY)부의 정보, 사용자 휴대장치의 고유키를 비교하는 작업을 수행하여 인증되지 않은 모듈인 경우 (610)과정으로 진행된다. 인증되지 않는다 함은 복호화 하였을 때 정상적인 데이터(Data)가 나오지 않거나, 사용자 정보 Data의 정보검증(예를 들어 CRC같은) 에서 맞지 않았을 때를 말한다. 이때에는 (609)과정에서 사용자의 불법사용을 위해 맞지않는 사용자 고유키 및 사용자 고유정보를 삭제할 것인지 묻는 내용을 디스플레이하고 사용자 어플리케이션 툴을 삭제하도록 한다. 사용자 어플리케이션 툴이 삭제된 후에는 도 5의 (501)과정으로 다시 진행하여 사용자 등록여부를 다시 확인한다.

이어서, (610)과정에서 사용자 고유키 및 사용자 고유정보가 일치되는 것이 확인되면 사용자 어플리케이션 툴에서 전송된 컨텐츠를 사용자의 고유키 및 사용자 고유정보를 이용하여 복호화한다. 만일, 전송시 문제가 발생하여 암호화된 컨텐츠가 올바르게 전송되지 않은 경우는 (612)과정으로 진행하여 복호화 불가능 처리를 화면에 출력하고 컨텐츠 제공서버로부터 (616)과정을 다시 수행하도록 한다.

이렇게 복호화된 컨텐츠는 사용자 어플리케이션 툴을 통해 실행되어 화면을 통해 출력되도록 한다(614).

즉, 컨텐츠 제공서버는 사용자의 인터넷 접속시, 사용자의 미등록시에 상기 무선단말의 고유정보를 이용하여 해당 사용자의 고유키를 생성 및 추출하기 위한 프로그램을 상기 접속한 사용자에게 전송하여 설치하도록 하고, 설치된 프로그램에 의해 상기 생성 및 전송된 사용자 고유키를 이용하여 해당 등록자를 등록한다.

상기와 같은 구성에 의해 본 발명의 특징에 따른 개인용 휴대장치에서 이미지 파일이나 음원파일, 동영상 파일등과 같은 컨텐츠의 정보보안 시스템이 이루어질 수 있다.

상술한 바와 같은 본 발명의 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 기록매체(씨디롬, 램, 롬, 플로피 디스크, 하드 디스크, 광자기 디스크 등)에 저장될 수 있다.

이상에서 설명한 본 발명은 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니고, 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하다는 것이 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 있어 명백할 것이다.

발명의 효과

상기한 바와 같은 본 발명은, 개인용 휴대장치의 응용 프로그램의 불법적인 복사 및 변형을 방지할 수 있기 때문에 개인용 휴대장치의 응용 프로그램 시장에서 저작권을 보호할 수가 있는 효과가 있다.

또한, 본 발명은, 개인용 휴대장치의 컨텐츠의 변형이나 복사로 인하여 발생할 수 있는 컨텐츠 정보의 유출을 방지할 수 있는 효과가 있다.

(57) 청구의 범위

청구항 1.

무선단말에서의 컨텐츠 저작권 관리 시스템에 있어서,

컨텐츠 제공서버로부터 사용자 어플리케이션 툴을 다운로드 받아 무선단말에 설치하며, 상기 무선단말의 고유 정보를 이용하여 무선단말 각각의 고유키를 생성하고, 생성된 사용자 고유키 정보를 컨텐츠 제공서버로 전송하기 위한 상기 무선단말; 및

상기 어플리케이션 툴을 통해 사용자 고유키 정보를 수신하여, 사용자 정보, 컨텐츠, 규칙 정보, 과금 정보를 저장하고, 사용자의 요구에 따라 컨텐츠를 사용자 고유키를 이용하여 암호화하여 중계국 및 기지국을 통해 전송하는 컨텐츠 제공서버

를 포함하는 무선단말에서의 컨텐츠 저작권 관리 시스템.

청구항 2.
제 1 항에 있어서,

상기 무선단말은,

상기 컨텐츠 제공서버와 상기 무선단말과의 전송과정을 통해 상기 컨텐츠 제공서버로부터 사용자 어플리케이션 툴을 다운로드 받아 무선단말에 설치하며, 상기 무선단말의 고유정보를 이용하여 해당 사용자의 고유키를 생성하기 위한 고유키 생성부;

상기 고유키 생성부를 통해 사용자 고유키 정보를 추출하기 위한 추출부; 및

상기 고유키 생성부로부터 다운받은 컨텐츠를 저장하기 위한 저장부

를 포함하는 무선단말에서의 컨텐츠 저작권 관리 시스템.

청구항 3.
제 1 항 또는 제 2 항에 있어서,

상기 컨텐츠 제공서버는,

상기 사용자 어플리케이션 툴을 통해 전송된 사용자 고유키 및 사용자 정보를 저장하기 위한 사용자 정보 저장부;

사용자에게 서비스하는 대상 컨텐츠를 저장하기 위한 컨텐츠 저장부;

사용자의 권한에 따른 저장권한, 사용기간 권한, 양도권한 등과 같은 규칙을 설정하는 규칙 저장부;

사용자의 컨텐츠 사용에 대한 권한으로, 컨텐츠에 대한 대가 처리 가능성 여부를 확인하고 과금 등의 처리를 수행하는 과금 저장부;

사용자에 의해 요청된 컨텐츠를 사용자의 고유키를 사용하여 암호화된 라이센스로 암호화하기 위한 암호화부; 및

상기 암호화수단에서 암호화된 라이센스 키(key)에 과금이나, 규칙, 사용자 고유키를 결합하여 암호화된 라이센스 키를 복호화하기 위한 라이센스 복호화 키를 생성하는 결합부

를 포함하는 무선단말에서의 컨텐츠 저작권 관리 시스템.

청구항 4.
제 1 항에 있어서,

상기 사용자 어플리케이션 툴은,

상기 컨텐츠 제공서버로부터 암호화된 컨텐츠를 다운로드 받을 시에, 규칙정보에 따라 다운로드 받는 해당 컨텐츠의 출력여부를 결정하는 것을 특징으로 하는 무선단말에서의 컨텐츠 저작권 관리 시스템.

청구항 5.
제 1 항에 있어서,

상기 사용자 어플리케이션 툴은,

상기 컨텐츠 제공서버로부터 암호화된 컨텐츠를 다운로드 받을 시에, 사용자 고유정보와, 상기 컨텐츠 제공서버로부터 암호화된 컨텐츠에 포함된 사용자 고유키와, 상기 무선단말에서 확인된 사용자 고유정보, 사용자 어플리케이션 툴

을 통해 추출된 사용자 고유키를 비교하여 다운로드 받은 암호화된 컨텐츠의 복호화 여부를 결정하는 것을 특징으로 하는 무선단말에서의 컨텐츠 저작권 관리 시스템.

청구항 6.
제 1 항에 있어서,

상기 사용자 어플리케이션 툴은,

초기 설치시와 해당 사용자 무선단말의 업그레이드나 정보변경시, 상기 사용 자 고유정보를 추가적으로 전송하는 것을 특징으로 하는 무선단말에서의 컨텐츠 저작권 관리 시스템.

청구항 7.
제 5 항에 있어서,

상기 사용자 고유키는,

무선단말의 중앙처리부(CPU)의 고유정보와, 메모리상의 고유정보 및 무선단말의 시리얼 정보 중 적어도 하나인 것을 특징으로 하는 무선단말에서의 컨텐츠 저작권 관리 시스템.

청구항 8.
제 5 항에 있어서,

상기 사용자 고유키는,

상기 무선단말의 전화번호를 포함하여 구성되는 것을 특징으로 하는 무선단말에서의 컨텐츠 저작권 관리 시스템.

청구항 9.
제 1 항 내지 제 8 항 중 어느 한 항에 있어서,

상기 암호화된 컨텐츠는,

사용자 정보, 사용자 기기정보 등이 포함되거나 혹은 해당 사용자 정보와 상 기 컨텐츠 제공서버를 통해 다른 사람에게 컨텐츠를 제공하고자 할 경우 특정 사용자의 전화번호와 같은 사용자 정보를 포함하는 헤더부와, 상기 컨텐츠 제공서버에서 사용자에게 제공하고자 하는 특정 컨텐츠로, 이미지 파일(GIF나 TIF 등), 음원 파일(MP3나 WMA, AAC, WAV 등), 영상 파일(DIVX나 WMV 등) 및 기타 형태의 컨텐츠를 사용하도록 하는 컨텐츠부와, 상기 무선단말로부터 얻어진 사용자 고유키를 이용하여 상기 컨텐츠부의 컨텐츠와 동일한 길이와 동일한 형태로 생성하기 위하여 매우 긴 주기의 난수열을 발생시켜 제작하고, 컨텐츠 키(key)부를 통하여 암호화된 컨텐츠부가 복호화되도록 하는 상기 컨텐츠 키(Key)부로 구성되는 것을 특징으로 하는 무선단말에서의 컨텐츠 저작권 관리 시스템.

청구항 10.
무선단말에서의 컨텐츠 저작권 관리 시스템에 있어서,

컨텐츠 제공서버와 무선단말과의 전송과정을 통해 상기 컨텐츠 제공서버로부터 사용자 어플리케이션 툴을 다운로드 받아 무선단말에 설치하며, 상기 무선단말의 고유정보를 이용하여 해당 사용자의 고유키를 생성하기 위한 고유키 생성수단;

상기 고유키 생성수단을 통해 사용자 고유키 정보를 추출하기 위한 추출수단; 및

상기 고유키 생성수단으로부터 다운받은 컨텐츠를 저장하기 위한 저장수단

을 포함하는 무선단말에서의 컨텐츠 저작권 관리 시스템.

청구항 11.
무선단말에서의 컨텐츠 저작권 관리 시스템에 있어서,

상기 사용자 어플리케이션 툴을 통해 전송된 사용자 고유키 및 사용자 정보를 저장하기 위한 사용자 정보 저장수단;

사용자에게 서비스하는 대상 컨텐츠를 저장하기 위한 컨텐츠 저장수단;

사용자의 권한에 따른 저장권한, 사용기간 권한, 양도권한 등과 같은 규칙을 설정하는 규칙 저장수단;

사용자의 컨텐츠 사용에 대한 권한으로, 컨텐츠에 대한 대가 처리 가능성 여부를 확인하고 과금 등의 처리를 수행하는 과금 저장수단;

사용자에 의해 요청된 컨텐츠를 사용자의 고유키를 사용하여 암호화된 라이센스로 암호화하기 위한 암호화수단; 및

상기 암호화수단에서 암호화된 라이센스 키(key)에 과금이나, 규칙, 사용자 고유키를 결합하여 암호화된 라이센스 키를 복호화하기 위한 라이센스 복호화 키를 생성하는 결합수단

을 포함하는 무선단말에서의 컨텐츠 저작권 관리 시스템.

청구항 12.
컨텐츠 저작권 관리 시스템에 적용되는 무선단말에서의 컨텐츠 저작권 관리 방법에 있어서,

사용자가 컨텐츠 제공서버에 접속시, 해당 사용자 무선단말로 사용자 어플리 케이션 툴을 설치하고, 상기 사용자 무선단말의 고유정보를 이용하여 생성된 사용자 고유키를 사용자 어플리케이션에서 추출하는 제 1 단계;

상기 사용자 고유키를 상기 컨텐츠 제공서버로 전송하는 제 2 단계;

사용자로부터 컨텐츠 다운로드 요청시, 해당 컨텐츠를 사용자 고유키를 통하여 암호화하고, 암호화된 컨텐츠 패키지를 생성하는 제 3 단계;

상기 암호화된 컨텐츠 패키지를 다시 사용자 고유정보를 통해서 암호화된 컨텐츠로 암호화하고, 암호화된 컨텐츠를 상기 무선단말로 전송하는 제 4 단계;

인증된 사용자의 무선단말에서 상기 암호화된 컨텐츠를 사용자 고유정보를 통해서 암호화된 컨텐츠 패키지로 복호화하는 제 5 단계; 및

상기 암호화된 컨텐츠 패키지를 사용자 고유키를 통해 컨텐츠로 복호화하고, 복호화된 컨텐츠를 상기 무선단말을 통해 출력하는 제 6 단계

를 포함하는 무선단말에서의 컨텐츠 저작권 관리 방법.

청구항 13.
제 12 항에 있어서,

상기 제 5 단계는,

상기 무선단말에서 다운로드 받은 암호화된 컨텐츠를 상기 사용자 어플리케이션 툴에서 추출한 사용자 고유키를 이용하여 복호화하고, 상기 암호화된 컨텐츠를 복호화하는 것을 특징으로 하는 무선단말에서의 컨텐츠 저작권 관리 방법.

청구항 14.
제 12 항에 있어서,

상기 암호화된 컨텐츠는,

상기 사용자 고유정보를 암호화된 컨텐츠의 헤더부에 추가하여 전송하는 것을 특징으로 하는 무선단말에서의 컨텐츠 저작권 관리 방법.

청구항 15.
제 12 항에 있어서,

상기 컨텐츠 제공서버는,

사용자의 인터넷 접속시, 사용자의 미등록시에 상기 무선단말의 고유정보를 이용하여 해당 사용자의 고유키를 생성 및 추출하기 위한 프로그램을 상기 접속한 사용자에게 전송하여 설치하도록 하고, 설치된 프로그램에 의해 상기 생성 및 전송된 사용자 고유키를 이용하여 해당 등록자를 등록하는 것을 특징으로 하는 무선단말에서의 컨텐츠 저작권 관리 시스템.

청구항 16.

프로세서를 구비한 컨텐츠 저작권 관리 시스템에,

사용자가 컨텐츠 제공서버에 접속시, 해당 사용자 무선단말로 사용자 어플리케이션 툴을 설치하고, 상기 사용자 무선단말의 고유정보를 이용하여 생성된 사용자 고유키를 사용자 어플리케이션에서 추출하는 제 1 기능;

상기 사용자 고유키를 상기 컨텐츠 제공서버로 전송하는 제 2 기능;

사용자로부터 컨텐츠 다운로드 요청시, 해당 컨텐츠를 사용자 고유키를 통하여 암호화하고, 암호화된 컨텐츠 패키지를 생성하는 제 3 기능;

상기 암호화된 컨텐츠 패키지를 다시 사용자 고유정보를 통해서 암호화된 컨텐츠로 암호화하고, 암호화된 컨텐츠를 상기 무선단말로 전송하는 제 4 기능;

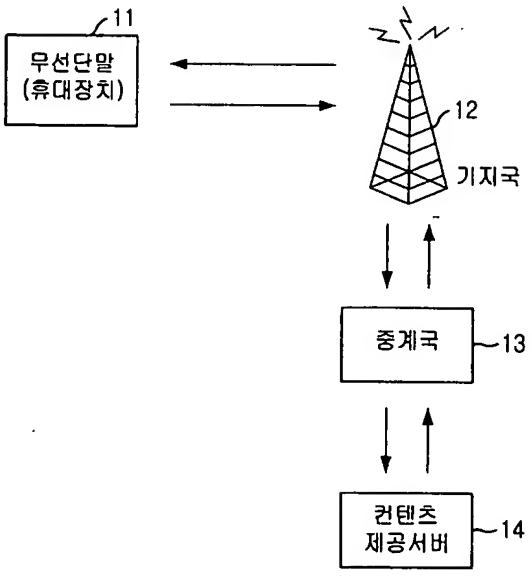
인증된 사용자의 무선단말에서 상기 암호화된 컨텐츠를 사용자 고유정보를 통해서 암호화된 컨텐츠 패키지로 복호화하는 제 5 기능; 및

상기 암호화된 컨텐츠 패키지를 사용자 고유키를 통해 컨텐츠로 복호화하고, 복호화된 컨텐츠를 상기 무선단말을 통해 출력하는 제 6 기능

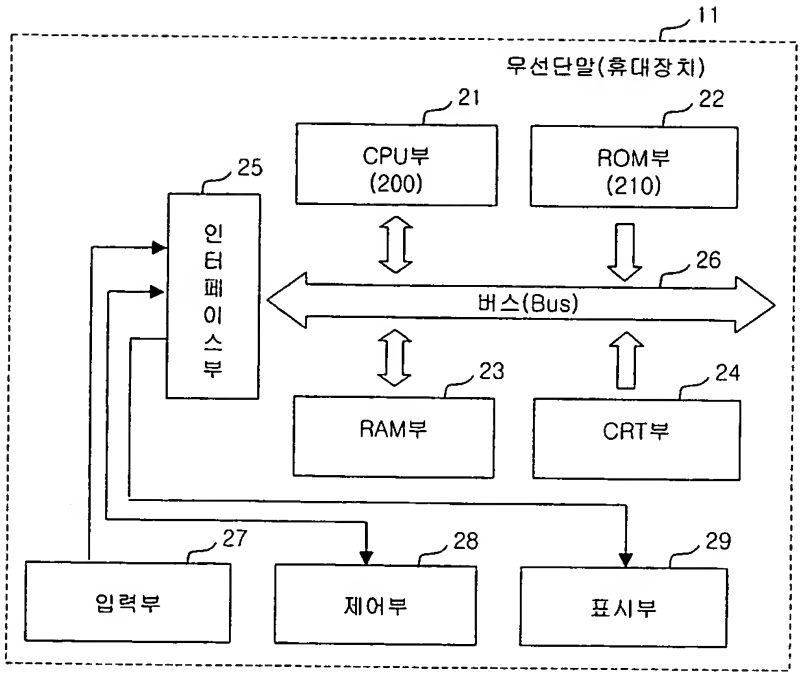
을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

도면

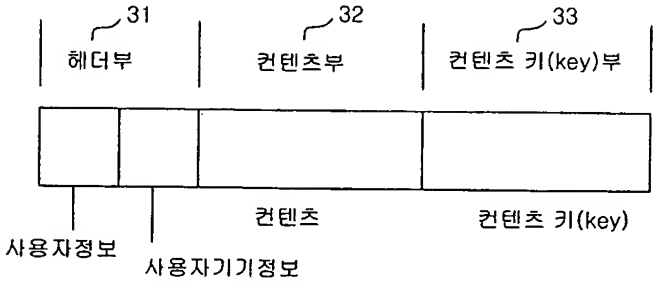
도면1



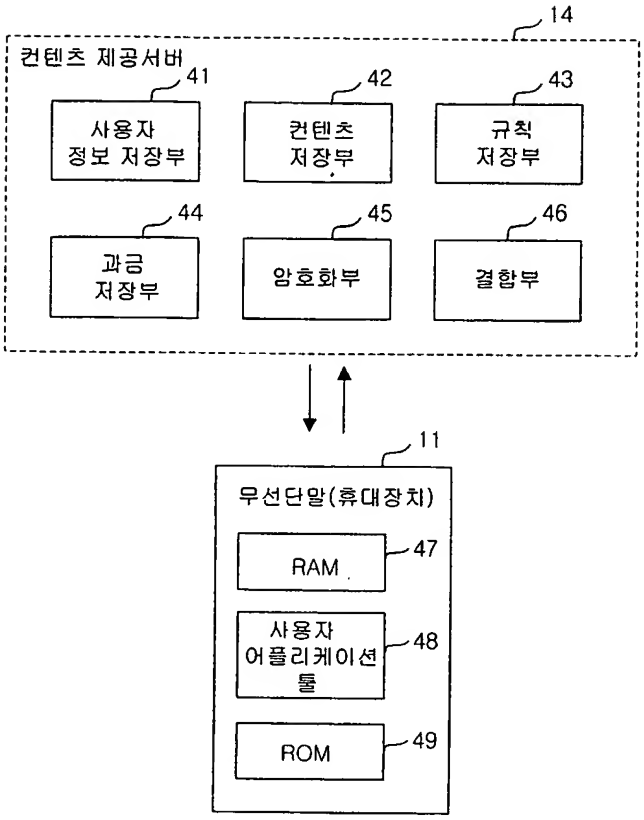
도면2


11
무선단말(휴대장치)
21
CPU부
(200)
22
ROM부
(210)
25
인터페이스부
26
버스(Bus)
23
RAM부
24
CRT부
27
입력부
28
제어부
29
표시부

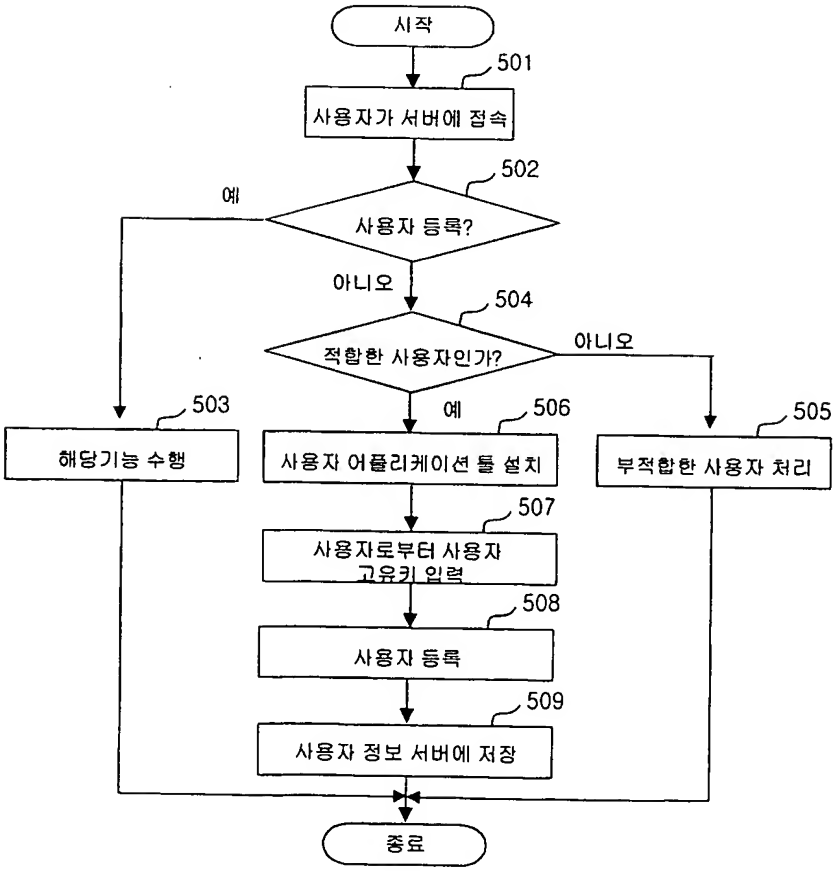
도면3


31
헤더부
32
컨텐츠부
33
컨텐츠 키(key)부
컨텐츠
컨텐츠 키(key)
사용자정보
사용자기기정보

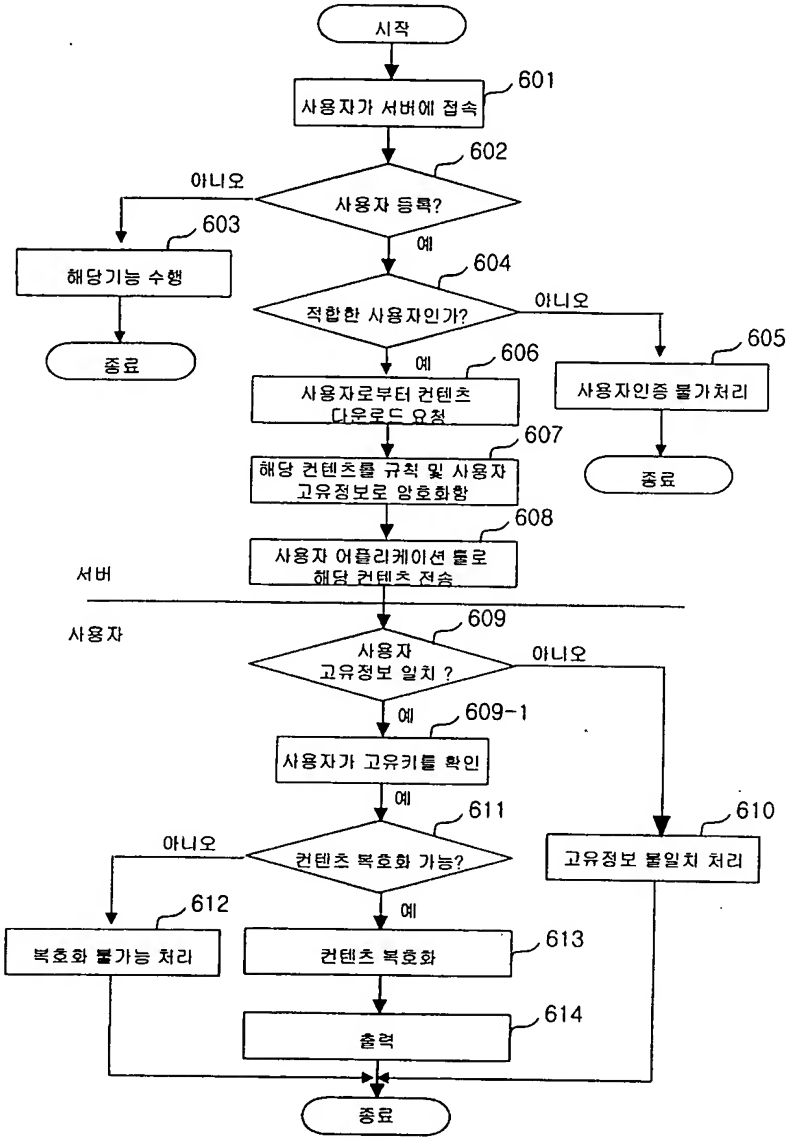
도면4


14
컨텐츠 제공서버
41
사용자 정보 저장부
42
컨텐츠 저장부
43
규칙 저장부
44
과금 저장부
45
암호화부
46
결합부
11
무선단말(휴대장치)
RAM
47
사용자 어플리케이션 툴
48
ROM
49

도면5


시작
501
사용자가 서버에 접속
502
사용자 등록?
예
아니오
504
적합한 사용자인가?
아니오
예
503
해당기능 수행
506
사용자 어플리케이션 툴 설치
505
부적합한 사용자 처리
507
사용자로부터 사용자 고유키 입력
508
사용자 등록
509
사용자 정보 서버에 저장
종료

도면6


시작
사용자가 서버에 접속
601
사용자 등록?
602
아니오
예
해당기능 수행
603
종료
적합한 사용자인가?
604
아니오
예
사용자인증 불가처리
605
종료
사용자로부터 컨텐츠 다운로드 요청
606
해당 컨텐츠를 규칙 및 사용자 고유정보로 암호화함
607
사용자 어플리케이션 툴로 해당 컨텐츠 전송
608
서버
사용자
사용자 고유정보 일치 ?
609
아니오
예
사용자가 고유키를 확인
609-1
예
컨텐츠 복호화 가능?
611
아니오
고유정보 불일치 처리
610
예
복호화 불가능 처리
612
컨텐츠 복호화
613
출력
614
종료